Storage Medium and Method for Storing Data Decrypting Algorithm

Background of the Invention

Field of the Invention

The present invention relates to a storage medium and a method for guaranteeing the security of stored data, and more specifically to an apparatus and method for decrypting encrypted data.

Description of the Related Art

In information processing technologies, there are several types of storage media for storing data. Conventional removable storage media are magnetic tapes, magnetic disks, magnet-optical disks, optical disks, etc., and new storage media are being introduced one after another. The information stored on such storage media may possibly be confidential, and are stored as encrypted data in many cases.

For example, in the conventional information processing system for decrypting encrypted information on a magnetic disk, encrypted data is read from the disk mounted into a drive unit, and then decrypted according to a predetermined decrypting algorithm. In another system not assigned the decrypting

STORAGE MEDIUM AND METHOD FOR STORING DATA DECRYPTING ALGORITHM

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to a storage medium and a method for guaranteeing the security of stored data, and more specifically to an apparatus and method for decrypting encrypted data.

[0003] 2. Description of the Related Art

[0004] In information processing technologies, there are several types of storage media for storing data. Conventional removable storage media are magnetic tapes, magnetic disks, magnet-optical disks, optical disks, etc., and new storage media are being introduced one after another. The information stored on such storage media may possibly be confidential, and are stored as encrypted data in many cases.

[0005] For example, in the conventional information processing system for decrypting encrypted information on a magnetic disk, encrypted data is read from the disk mounted into a drive unit, and then decrypted according to a predetermined decrypting algorithm. In another system not assigned the decrypting algorithm, data cannot be decrypted, thereby guaranteeing the security of the data on the disk.

[0006] However, the above described conventional security guarantee method has the following problems.

[0007] Because an algorithm for decrypting data on a disk is assigned a system, once the algorithm has been decrypted, data can be read through the algorithm by other systems that don't assign the decrypting algorithm.

[0008] Furthermore, since an encrypted disk is generated to be applied to the decrypting algorithm stored in a system, it is necessary to disclose the algorithm to the disk generator to encrypt the data. Therefore, a third party may obtain the disclosed algorithm and be able to decrypt the encrypted data.

[0009] Since a decrypting algorithm is simple, the security of encrypted data cannot be guaranteed once the algorithm has been decrypted.

SUMMARY OF THE INVENTION

[0010] The present invention aims at providing a storage medium and method for guaranteeing the security of encrypted data.

[0011] The storage medium according to the present invention has a data area unit and an algorithm area unit.

[0012] The data area unit stores encrypted data.

[0013] The algorithm area unit stores an algorithm for decrypting data in the data area unit.

[0014] Since the storage medium according to the present invention stores both encrypted data and the algorithm for decrypting the data, different data encrypting algorithm can be applied to each storage medium. Therefore, even if the security is violated by disclosure of one decrypting algorithm, the security of the data on another storage medium can be maintained.

[0015] The above described data area unit is provided in a portion accessible by the user on the storage medium. The above described algorithm area unit is provided in a portion inaccessible by the user on the storage medium. With this configuration, the user cannot directly access the decrypting algorithm for the data on the storage medium. As a result, there is little possibility that the above described decrypting algorithm may be disclosed by the user, also the data contents on the medium is protected from being intentionally disclosed by rewriting of the data in the algorithm area unit.

[0016] The decryption is performed using the algorithm in the above described algorithm area unit by receiving and using a decrypting key from outside an external storage device into which the storage medium is mounted, for example, from an information processing unit connected to an external storage device. Thus, the security of the information can be further improved.

[0017] The decryption of the data can be performed by a request from an information processing device connected to an external storage device in which the storage medium is mounted to another device, for example, a server connected through a network. With this configuration, the data decrypting algorithm can also be encrypted, thereby further improving the security for the data stored on the storage medium.

[0018] Thus, according to the present invention, both of the encrypted data and the decrypting algorithm can be stored on the storage medium, and the encrypting algorithm can be altered for each piece of data or each storage medium, thus improving the security of the data stored on the storage medium.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] **FIG. 1** shows the principle of the present invention;

[0020] **FIG. 2** shows the configuration according to the first embodiment;

[0021] **FIG. 3** shows the storage areas of a storage medium;

[0022] **FIG. 4** is a flowchart showing the process of the decrypting mechanism;

[0023] **FIG. 5** shows the configuration according to the second embodiment;

[0024] **FIG. 6** shows the configuration according to the third embodiment; and

[0025] **FIG. 7** is a flowchars showing the process of a device driver.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0026] **FIG. 1** shows the principle of the storage medium according to the present invention. A storage medium **1** shown in **FIG. 1** comprises a data area unit **2** storing encrypted data and an algorithm area unit **3** storing an algorithm for decrypting the data.

[0027] Since data and its decrypting algorithm are stored as a pair on the same storage medium, specific encrypting and decrypting methods can be applied to each piece of data